

ON COMPOSITENESS OF SPECIAL TYPES OF INTEGERS

YU TSUMURA

ABSTRACT. In paper on a classification of Lehmer triples, Juricevic conjectured that there are infinitely many primes of special form. We disprove one of his conjectures and consider the other one.

1. INTRODUCTION

In paper [1], Juricevic proved a theorem on a classification of Lehmer triples under the assumption of the following two conjectures.

Conjecture 1.1. *There are infinitely many prime numbers $p > 5$ such that*

$$T(p) := \frac{1}{5} \left((1 + \sqrt{5}) \left(\frac{3 + \sqrt{5}}{2} \right)^{2p} + (1 - \sqrt{5}) \left(\frac{3 - \sqrt{5}}{2} \right)^{2p} + 3 \right)$$

is a prime number.

Conjecture 1.2. *There are infinitely many prime numbers $p > 5$ such that*

$$Y(p) := \frac{1}{3} \left((1 + \sqrt{3}) \left(2 + \sqrt{3} \right)^{2p} + (1 - \sqrt{3}) \left(2 - \sqrt{3} \right)^{2p} + 1 \right)$$

is a prime number.

In this article we discuss those two types of integers. Actually, we disprove Conjecture 1.2 and also show that there are infinitely many composite numbers $T(p)$. The proofs are elementary. We use simple properties of second-order linear recurrence sequences.

2. LEMMAS

Here we prove some basic properties of second-order linear recurrence sequences.

First of all, let us set up the situation. Let $P, Q \in \mathbb{Z} \setminus \{0\}$ and $X^2 - PX + Q = (X - \alpha)(X - \beta)$. Hence $\alpha + \beta = P$ and $\alpha\beta = Q$. Let us define $V_n(P, Q) = \alpha^n + \beta^n$ for integer $n \geq 0$. Note that we have $V_0(P, Q) = 2$ and $V_1(P, Q) = P$.

2010 *Mathematics Subject Classification.* Primary 11A51; Secondary 11B51.

Key words and phrases. Lehmer triples, linear recurrence sequences, compositeness.

For simplicity, let V_n denote $V_n(P, Q)$ when P, Q are understood. It is easy to show the next lemma and we omit the proof. The reader will find many properties of second-order linear recurrence sequences, for example, in [2].

Lemma 2.1. *For $P, Q \in \mathbb{Z} \setminus \{0\}$ and $V_n = V_n(P, Q)$, we have*

$$V_n = PV_{n-1} - QV_{n-2}.$$

Now take $t_0, t_1 \in \mathbb{Z} \setminus \{0\}$. Let $\gamma = t_1 - t_0\beta$ and $\delta = t_1 - t_0\alpha$.

Lemma 2.2. *We have*

$$\gamma\alpha^n + \delta\beta^n = t_1V_n - Qt_0V_{n-1}.$$

Proof. We have

$$\begin{aligned} \gamma\alpha^n + \delta\beta^n &= t_1\alpha^n - t_0\alpha^n\beta + t_1\beta^n - t_0\alpha\beta^n \\ &= t_1(\alpha^n + \beta^n) - t_0\alpha\beta(\alpha^{n-1} + \beta^{n-1}) \\ &= t_1V_n - t_0QV_{n-1}. \end{aligned}$$

□

3. ALL $Y(p)$ ARE COMPOSITE.

Now we disprove Conjecture 1.2.

Theorem 3.1. *$Y(p)$ is composite for all primes p .*

Proof. We use the lemmas with $P = 4, Q = 1, t_0 = 1, t_1 = 3$. For these choices, we have $\alpha = 2 + \sqrt{3}, \beta = 2 - \sqrt{3}, \gamma = 1 + \sqrt{3}$ and $\delta = 1 - \sqrt{3}$. By Lemma 2.2, we have for integer n

$$3V_n - V_{n-1} = \gamma\alpha^n + \delta\beta^n = (1 + \sqrt{3}) \left(2 + \sqrt{3}\right)^n + (1 - \sqrt{3}) \left(2 - \sqrt{3}\right)^n.$$

Hence we have for prime p

$$(3.1) \quad Y(p) = \frac{1}{3}(3V_{2p} - V_{2p-1} + 1).$$

Now we prove that $Y(p)$ is divisible by 3 when $p \equiv 5 \pmod{6}$ and is divisible by 13 when $p \equiv 1 \pmod{6}$. Since $Y(2) = 3 \cdot 59$ and $Y(3) = 23 \cdot 107$, this shows that $Y(p)$ is composite for all primes p .

We calculate $V_n \pmod{9}$ using Lemma 2.1, that is, $V_n = 4V_{n-1} - V_{n-2}$. The result is the following list.

n	$V_n \pmod{9}$
0	2
1	4
2	5
3	7
4	5
5	4
6	2
7	4

Now since V_n is calculated from the previous two terms, we see from the list that $V_n \pmod{9}$ has period 6.

Let $p \equiv 5 \pmod{6}$. Then $2p \equiv 4 \pmod{6}$ and $2p - 1 \equiv 3 \pmod{6}$. Hence by (3.1) we have

$$3Y(p) \equiv 3V_4 - V_3 + 1 \equiv 3 \cdot 5 - 7 + 1 \equiv 0 \pmod{9}.$$

Hence 3 divides $Y(p)$ when $p \equiv 5 \pmod{6}$.

Next we calculate $V_n \pmod{13}$ and obtain the following list.

n	$V_n \pmod{13}$	n	$V_n \pmod{13}$
0	2	7	9
1	4	8	12
2	1	9	0
3	0	10	1
4	12	11	4
5	9	12	2
6	11	13	4

We see that $V_n \pmod{13}$ has period 12.

Let $p \equiv 1 \pmod{6}$. Then we have $2p \equiv 2 \pmod{12}$ and $2p - 1 \equiv 1 \pmod{12}$. Hence by (3.1) we have

$$3Y(p) \equiv 3V_2 - V_1 + 1 \equiv 3 \cdot 1 - 4 + 1 \equiv 0 \pmod{13}.$$

It follows that $Y(p)$ is divisible by 13 when $p \equiv 1 \pmod{6}$.

As noted above, this shows that $Y(p)$ is composite for all primes p . \square

4. THERE ARE INFINITELY MANY COMPOSITE $T(p)$.

Let us consider $T(p)$. Now $T(p)$ is not composite for all primes p . For example, $T(p)$ is prime for $p = 2, 5, 809$. (These are the only primes the author found.)

Although we neither prove nor disprove Conjecture 1.1, we can show that there are infinitely many primes p such that $T(p)$ is composite.

Theorem 4.1. *Let p be a prime number.*

- (1) If $p \equiv 1 \pmod{5}$, then $T(p)$ is divisible by 5.
 (2) If $p \equiv 3 \pmod{5}$, then $T(p)$ is divisible by 11.
 (3) If $p \equiv 2 \pmod{15}$, then $T(p)$ is divisible by 31.

Proof. We use the above lemmas with $P = 3$, $Q = 1$, $t_0 = 2$, $t_1 = 4$. With these values, we have $\alpha = (3 + \sqrt{5})/2$, $\beta = (3 - \sqrt{5})/2$, $\gamma = 1 + \sqrt{5}$ and $\delta = 1 - \sqrt{5}$. By Lemma 2.2, it follows that for integer n

$$4V_n - 2V_n = \gamma\alpha^n + \delta\beta^n = (1 + \sqrt{5}) \left(\frac{3 + \sqrt{5}}{2} \right)^n + (1 - \sqrt{5}) \left(\frac{3 - \sqrt{5}}{2} \right)^n.$$

Hence we have

$$(4.1) \quad T(p) = \frac{1}{5}(4V_{2p} - 2V_{2p-1} + 3)$$

We calculate $V_n \pmod{25}$ using Lemma 2.1, that is, $V_n = 3V_{n-1} - V_{n-2}$.

n	$V_n \pmod{25}$	n	$V_n \pmod{25}$
0	2	6	22
1	3	7	18
2	7	8	7
3	18	9	3
4	22	10	2
5	23	11	3

Since V_n is calculated from the previous two terms, we see that $V_n \pmod{25}$ has period 10. When $p \equiv 1 \pmod{5}$, we have $2p \equiv 2 \pmod{10}$ and $2p-1 \equiv 1 \pmod{10}$. So by (4.1) it follows that

$$5T(p) \equiv 4V_2 - 2V_1 + 3 \equiv 4 \cdot 7 - 2 \cdot 3 + 3 \equiv 0 \pmod{25}.$$

Therefore $T(p)$ is divisible by 5 when $p \equiv 1 \pmod{5}$.

Next, we calculate $V_n \pmod{11}$ and obtain the following list.

n	$V_n \pmod{11}$
0	2
1	3
2	7
3	7
4	3
5	2
6	3

Hence we see that $V_n \pmod{11}$ has period 5. When $p \equiv 3 \pmod{5}$, we have $2p \equiv 1 \pmod{5}$ and $2p-1 \equiv 0 \pmod{5}$. So it follows from (4.1) that

$$5T(p) \equiv 4V_1 - 2V_0 + 3 \equiv 4 \cdot 3 - 2 \cdot 2 + 3 \equiv 0 \pmod{11}.$$

Therefore $T(p)$ is divisible by 11 when $p \equiv 3 \pmod{5}$.

Finally, we calculate $V_n \pmod{31}$ and obtain the following list.

n	$V_n \pmod{31}$	n	$V_n \pmod{31}$
0	2	9	12
1	3	10	30
2	7	11	16
3	18	12	18
4	16	13	7
5	30	14	3
6	12	15	2
7	6	16	3
8	6		

Hence we see that $V_n \pmod{31}$ has period 15. When $p \equiv 2 \pmod{15}$, we have $2p \equiv 4 \pmod{15}$ and $2p - 1 \equiv 3 \pmod{15}$. So it follows from (4.1) that

$$5T(p) \equiv 4V_4 - 2V_3 + 3 \equiv 4 \cdot 16 - 2 \cdot 18 + 3 \equiv 0 \pmod{31}.$$

Hence $T(p)$ is divisible by 31 when $p \equiv 2 \pmod{15}$ □

By equation (4.1), it is easy to see that $T(p)$ goes to infinity as p tends to infinity. Also, by Dirichlet's theorem on arithmetic progressions, there are infinitely many primes p of each of the three forms in Theorem 4.1. Therefore, it follows that there are infinitely many prime numbers p such that $T(p)$ is composite.

According to Theorem 4.1, if $T(p)$ is prime for $p > 5$, then p is congruent to one of 7, 19, 29 $\pmod{30}$. However, there is no prime q so that q divides $T(p)$ for all p congruent to any one of 7, 19, 29 $\pmod{30}$. This can be easily seen by taking two primes in the same class and observing that the greatest common divisor of the two $T(p)$ s is equal to 1.

For other classes of p , there might be a trivial divisor as in Theorem 4.1 and can be proved by the same method. For example, we can prove the following theorem.

Theorem 4.2. (1) If $p \equiv 7 \pmod{65}$, then $T(p)$ is divisible by 131.
(2) If $p \equiv 29 \pmod{35}$, then $T(p)$ is divisible by 71.

Proof. The method of proof is exactly the same as that of in the proof of Theorem 4.1. Also since periods are larger, we just sketch the proof.

One finds that $T(p) \pmod{131}$ has period 65. When $p \equiv 7 \pmod{65}$, we have $2p \equiv 14 \pmod{65}$ and $2p - 1 \equiv 13 \pmod{65}$. By direct calculations we see that $V_{14} \equiv 103 \pmod{131}$ and $V_{13} \equiv 11 \pmod{131}$. Hence it follows from (4.1) that

$$5T(p) \equiv 4V_{14} - 2V_{13} + 3 \equiv 4 \cdot 103 - 2 \cdot 11 + 3 \equiv 0 \pmod{131}.$$

Hence $T(p)$ is divisible by 131.

The proof of the second statement is similar. We see that $T(p) \pmod{71}$ has period 35. When $p \equiv 29 \pmod{35}$, we have $2p \equiv 23 \pmod{35}$ and $2p-1 \equiv 22 \pmod{35}$. By direct calculations we see that $V_{23} \equiv 22 \pmod{71}$ and $V_{21} \equiv 10 \pmod{71}$. Hence it follows from (4.1) that

$$5T(p) \equiv 4V_{23} - 2V_{22} + 3 \equiv 4 \cdot 22 - 2 \cdot 10 + 3 \equiv 0 \pmod{71}.$$

Therefore $T(p)$ is divisible by 71. \square

Although we can find more similar divisibility properties, we refrain from stating them. Finally, one can notice that we do not use the fact that p is prime. All the arguments hold if one allows p to be composite.

REFERENCES

- [1] Robert Juricevic, *Classifying Lehmer triples*, Acta Arith. **137** (2009), no. 3, 207–232. MR MR2496461
- [2] Paulo Ribenboim, *The little book of bigger primes*, second ed., Springer-Verlag, New York, 2004. MR MR2028675 (2004i:11003)

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY 150 NORTH UNIVERSITY STREET, WEST LAFAYETTE, INDIANA 47907-2067
E-mail address: ytsumura@math.purdue.edu